65526-US
TOK/mk

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月　７日

出願番号
Application Number: 特願２００２－２２９９４９

[ST.10/C]: [ＪＰ２００２－２２９９４９]

出願人
Applicant(s): 株式会社デンソー

２００３年　５月　２日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０３１３７０

【書類名】　特許願
【整理番号】　PNID4105
【提出日】　平成14年 8月 7日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 3/06
【発明者】
　【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
　【氏名】　藤本　英俊
【発明者】
　【住所又は居所】　愛知県刈谷市昭和町１丁目１番地　株式会社デンソー内
　【氏名】　木村　匡宏
【特許出願人】
　【識別番号】　000004260
　【氏名又は名称】　株式会社デンソー
【代理人】
　【識別番号】　100082500
　【弁理士】
　【氏名又は名称】　足立　勉
　【電話番号】　052-231-7835
【手数料の表示】
　【予納台帳番号】　007102
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9004766
【プルーフの要否】　要

【書類名】明細書

【発明の名称】　データの暗号化方法及び装置、データの復号化方法及び装置、プログラム

【特許請求の範囲】

【請求項１】

対象となるデータに対し、所定の暗号化単位データ長毎に、その暗号化単位データ長の内で実際に暗号化を施す比率を示す所定の暗号化比率に基づいて、暗号化前後のデータ長が不変の暗号化を施すことを特徴とするデータの暗号化方法。

【請求項２】

請求項１に記載のデータの暗号化方法において、

前記所定の暗号化比率は複数種類存在し、

それら複数種類の暗号化比率を所定の順番で適用して暗号化することを特徴とするデータの暗号化方法。

【請求項３】

請求項２に記載のデータの暗号化方法において、

前記所定の順番で適用して暗号化する際、同じ種類の暗号化比率を所定回数連続して適用して暗号化することを特徴とするデータの暗号化方法。

【請求項４】

請求項１～３のいずれかに記載のデータの暗号化方法において、

前記所定の暗号化比率に基づいて部分的に暗号化する際、前記所定の暗号化単位データ長の内の所定位置から暗号化を開始することを特徴とするデータの暗号化方法。

【請求項５】

請求項４に記載のデータの暗号化方法において、

前記所定の暗号化開始位置は複数種類存在し、

前記暗号化比率と前記暗号化開始位置の組合せによる複数パターンを所定の順番で適用して暗号化することを特徴とするデータの暗号化方法。

【請求項６】

暗号化対象となるデータを入力する機能、

その入力したデータに対して、前記請求項１～５の何れかに記載の暗号化方法を用いて暗号化する機能、

暗号化したデータを外部へ出力する機能

を備えることを特徴とするデータの暗号化装置。

【請求項７】

コンピュータに、

暗号化対象となるデータを入力する機能、

その入力したデータに対して、前記請求項１～５の何れかに記載の暗号化方法を用いて暗号化する機能、

暗号化したデータを外部へ出力する機能

を実現させるためのプログラム。

【請求項８】

所定の暗号化単位データ長毎にその暗号化単位データ長の内で実際に暗号化を施す比率を示す所定の暗号化比率に基づいて暗号化前後のデータ長が不変の暗号化が施されたデータに対し、その暗号化のルールに基づいて復号化することを特徴とするデータの復号化方法。

【請求項９】

請求項８に記載のデータの復号化方法において、

複数種類存在する前記所定の暗号化比率が所定の順番で適用されて暗号化されたデータを、その暗号化比率の種類及び適用順番を含む暗号化ルールに基づいて復号化することを特徴とするデータの復号化方法。

【請求項１０】

請求項９に記載のデータの復号化方法において、

同じ種類の暗号化比率が所定回数連続して適用されて暗号化されたデータを、その連続する所定回数も含む暗号化ルールに基づいて復号化することを特徴とするデータの復号化方法。

【請求項１１】

請求項８～１０のいずれかに記載のデータの復号化方法において、

前記所定の暗号化単位データ長の内の所定位置から前記所定の暗号化比率に基

づく暗号化がなされたデータを、その暗号化開始位置も含む暗号化ルールに基づいて復号化することを特徴とするデータの復号化方法。

【請求項１２】

請求項１１に記載のデータの復号化方法において、

前記暗号化比率と複数種類存在する前記暗号化開始位置の組合せによる複数パターンを所定の順番で適用して暗号化されたデータを、その複数パターンが適用された順番も含む暗号化ルールに基づいて復号化することを特徴とするデータの復号化方法。

【請求項１３】

復号化対象となるデータを入力する機能、

その入力したデータに対して、前記請求項８～１２の何れかに記載の復号化方法を用いて復号化する機能、

その復号化したデータを外部へ出力する機能

を備えることを特徴とするデータの復号化装置。

【請求項１４】

コンピュータに、

復号化対象となるデータを入力する機能、

その入力したデータに対して、前記請求項８～１２の何れかに記載の復号化方法を用いて復号化する機能、

その復号化したデータを外部へ出力する機能

を実現させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データの暗号化や復号化等の技術に関する。

【０００２】

【従来の技術】

従来より、例えば地図表示装置や経路案内装置など、地図データを利用して所定の処理を実行する装置が知られている。例えばカーナビゲーション装置は地図

表示や経路案内を行うため、その代表的な装置として考えられる。このような装置で用いられる地図データはＤＶＤ－ＲＯＭやＣＤ－ＲＯＭあるいはＨＤＤ等の記録媒体に記録されて利用者に提供されている。

【０００３】

このような地図データに対しては、不正にコピーされないよう暗号化して記録しておくことが考えられる。但し、全てのデータを暗号化すると解読処理の際に必要なメモリが多くなり処理時間も長くなるため、実用的でない。そこで、例えば、保護対象のデータがヘッダ情報とコンテンツデータとから構成されている場合に、ヘッダ情報には復号に相対的に時間のかかる複雑な暗号化を施し、コンテンツデータには復号に相対的に時間のかからない復号化を施す技術が知られている（例えば、特許文献１参照。）。また、コンテンツデータについては暗号化せず、ボリュームディスクリプタ又はヘッダ情報のみを暗号化する技術も知られている（例えば、特許文献２参照。）。この特許文献２に開示された技術においては、利用時の高速化のため、例えば画像や音声等のコンテンツデータは暗号化しないようにしている。

【０００４】

特許文献１：特開２０００－３４１２６６号公報

特許文献２：特表２００１－５１７８３３号公報

【０００５】

【発明が解決しようとする課題】

しかしながら、特許文献２に開示された従来技術の場合には、ヘッダ情報やボリュームディスクリプタのみ暗号化され、コンテンツデータについて何ら暗号化されていないため、そのデータはそのまま利用可能な状態でコピーされてしまう可能性がある。もちろん、ヘッダ情報等が暗号化されているため、全く同様に使用することはできなくても、データの内容自体を知ることはできるため、問題がある。また、特許文献１に開示された従来技術の場合には、暗号化の強度が異なってはいるものの、保護対象のデータ全てに対して暗号化を施すものであり、さらに、ヘッダ情報とコンテンツデータを区別して強度の異なる暗号化を施すということは、保護対象のデータ中においてヘッダ情報がどれかということを解析し

て判断する必要がある。したがって、そのような解析の手間は発生する。

【０００６】

そこで、本発明は、不正コピーへの対策を講じながら、復号処理に要する時間を極力低減させる暗号化技術等を提供することを目的とする。

【０００７】

【課題を解決するための手段及び発明の効果】

（１）暗号化に関して

①請求項１記載の暗号化方法は、対象となるデータを、所定の暗号化単位データ長毎に、所定の暗号化比率に基づいて、暗号化前後のデータ長が不変の暗号化を施すものである。

【０００８】

従来はヘッダ情報のみを暗号化することなどが考えられているが、例えばコンテンツデータについて何ら暗号化されていなければ、そのデータはそのまま利用可能な状態でコピーされてしまう可能性がある。もちろん、ヘッダ情報が暗号化されているため、全く同様に使用することはできなくても、データの内容自体を知ることはできるため、問題がある。

【０００９】

それに対して本発明の場合には、所定の暗号化単位データ中に暗号化されないデータが残存していたとしても、一部は暗号化されているため、所定の暗号化単位データ全体が知られないとデータ内容についての有効利用ができない。

また、データ内容に応じて暗号化するということは、例えばヘッダ情報がどれかということを解析して判断する必要があるが、本発明の場合には、暗号化単位データ長と暗号化比率に基づく所定の暗号化ルールに基づいて暗号化するため、データ内容を意識することなく、つまり、どこがヘッダ部分でどこがコンテンツ部分かといった区別をすることなく、所定の暗号化ルールに基づいて機械的に暗号化するだけでよい。そのため、処理負荷の低減が期待できる。

【００１０】

そして、暗号化前後でデータ長が不変であるため、復号化する場合には、復号するために用いる暗号鍵と暗号化のルール（この場合であれば暗号化比率）を情

報として把握していれば、容易に復号化できる。

なお、暗号化の対象データとしては例えば地図データなどが考えられるが、地図に限定はしない。地図データの場合はベクトルデータがメインとなるが、例えば画像データや音声データ、あるいはテキストデータであってもよい。

【００１１】

また、「所定の暗号化単位データ長」に関しては、次の観点で決まる所定範囲内とすることが考えられる。つまり、暗号化単位データ長があまり長いと、その内の暗号化されていない平文のデータ部分が長く連続してしまう可能性があり、その場合は、その連続した平文のデータがそのまま不正コピーされた場合に実用的な意味を持ってしまうと、適切な暗号化とは言えなくなる。したがって、不正コピーされた場合において、平文データのみでは実質的に意味をなさない、あるいは利用が非常に制限されてしまうような上限を設定することが好ましい。これは、暗号化対象のデータ内容によっても異なる可能性はある。例えば地図データ等を考えると、ある程度広い範囲に対する地図データが平文で存在しなければ、不正コピーしても利用が非常に制限されてしまう。また、画像データや音声データに関しては、部分的に平文データが存在しても、暗号化部分が存在することによって、再生時にいわゆるスクランブルがかかったような状態となり、視聴に耐えないような状態となる。したがって、このような観点で暗号化単位データ長の上限は決めることができる。一方、不正コピーによる実質的被害の防止のためには暗号化単位データ長は短い方がよい。しかし、短くし過ぎると処理負荷が増大するため、それらのバランスを考える必要がある。したがって、要求される暗号化強度に応じた適切な暗号化単位データ長を採用すればよい。

【００１２】

②請求項２に示すように、暗号化比率が複数種類存在する場合には、それら複数種類の暗号化比率を所定の順番で適用して暗号化してもよい。例えば２５％・５０％・７５％という３種類の暗号化比率をその順番で繰り返し適用してもよい。さらには、請求項３に示すように、同じ種類の暗号化比率を所定回数連続して適用してもよい。例えば２５％→２５％→５０％→５０％→７５％→７５％→２５％……というように、各暗号化比率をそれぞれ２回ずつ繰り返すようにしても

よい。

【００１３】

また、暗号化は必ずしも対象データの先頭から施さなくてはならないわけではなく、請求項４に示すように、所定の暗号化単位データ長の内の所定位置から暗号化を開始してもよい。例えば先頭から２５％位置から開始したり、先頭から５０％位置、あるいは先頭から７５％位置から開始する、といったことである。もちろん、先頭から０％位置、つまり先頭から暗号化しても当然よい。

【００１４】

このように、暗号化する際のルールが、暗号化比率の種類や暗号化開始位置によって複数パターン存在することにより、暗号化の強度が向上する。暗号化の強度を向上させる観点からすれば、例えば請求項５に示すように、暗号化比率と複数の暗号化開始位置の組合せによる複数パターンを所定の順番で適用して暗号化することは好ましい。もちろん、「複数種類」の暗号化比率と「複数」の暗号化開始位置の組合せによる複数パターンであれば、さらに多くのパターンが形成される。

【００１５】

なお、当然であるが、復号化に際しては、このような暗号化の際に適用した暗号化ルールを把握した上で実行するのであるが、この暗号化ルールを適用する場合においても、やはり従来技術のようなデータの内容を把握する必要はない。つまり、どの部分がヘッダ情報であるかといった考慮は不要であり、データ長を把握して機械的に暗号化すればよいため、処理負荷は相対的に低減することが期待できる。

【００１６】

③また、このような暗号化方法を用いて暗号化を行うデータの暗号化装置としては、請求項６に示すような構成が考えられる。つまり、暗号化対象となるデータを入力し、その入力したデータに対して、上述の暗号化方法を用いて暗号化し、その暗号化したデータを外部へ出力するのである。暗号化したデータを外部へ出力する場合、その出力された暗号化データは例えばＤＶＤ－ＲＯＭ等の記録媒体に記録されたり、ネットワークを介して送信されたりすることが考えられる。

【００１７】

④また、このような暗号化処理をコンピュータが実行するプログラムとしては、請求項７に示すようなものが考えられる。このようなプログラムの場合、例えば、フレキシブルディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ハードディスク、ＲＯＭ、ＲＡＭ等のコンピュータ読み取り可能な記録媒体に記録し、必要に応じてコンピュータシステムにロードして起動することにより用いることができ、また、ネットワークを介してロードして起動することにより用いることもできる。

【００１８】

（２）復号化に関して

①一方、上述した請求項１に記載の暗号化方法によって暗号化されたデータを復号する方法としては、請求項８に示すものが考えられる。つまり、所定の暗号化単位データ長毎にその暗号化単位データ長の内で実際に暗号化を施す比率を示す所定の暗号化比率に基づいて暗号化前後のデータ長が不変の暗号化が施されたデータに対し、その暗号化ルールに基づいて復号化するのである。

【００１９】

暗号化前後でデータ長が不変であるため、復号化する場合には、復号するために用いる暗号鍵と暗号化のルール（この場合であれば暗号化比率）を情報として把握していれば、容易に復号化できる。

②また、請求項２～５に記載の暗号化方法によって暗号化されたデータを復号する方法としては、それぞれ請求項９～１２に示すものが考えられる。それぞれの暗号化ルールに基づいて復号化することができる。例えば暗号化比率に加え、請求項９であれば適用順番、請求項１０であれば連続回数、請求項１１であれば暗号化開始位置、請求項１２であれば適用順番も含む暗号化ルールに基づいて復号化する。

【００２０】

③また、このような復号化方法を用いて復号化を行うデータの復号化装置としては、請求項１３に示すような構成が考えられる。つまり、復号化対象となるデータを入力し、その入力したデータに対して、上述の復号化方法を用いて復号化し、その復号化したデータを外部へ出力する。この出力された復号化データは、

例えばそのデータを用いて所定のアプリケーション処理を実行する機器に内蔵された記録媒体等に記録されたりする。

【００２１】

④また、このような復号化処理をコンピュータが実行するプログラムとしては、請求項１４に示すようなものが考えられる。

【００２２】

【発明の実施の形態】

以下、本発明が適用された実施例について図面を用いて説明する。なお、本発明の実施の形態は、下記の実施例に何ら限定されることなく、本発明の技術的範囲に属する限り、種々の形態を採り得ることは言うまでもない。

【００２３】

図１（ａ）は、データ暗号化装置１の概略構成図、図１（ｂ）は、データ復号化装置２の概略構成図である。

データ暗号化装置１は、外部からのデータを入力するための入力部１１と、その入力部１１を介して入力したデータに対して暗号化を施す暗号化部１２と、その暗号化部１２にて暗号化されたデータを外部へ出力する出力部１３とを備えている。本実施例では、データ格納部３に格納された平文の地図データをデータ暗号化装置１によって暗号化し、その暗号化した地図データをＤＶＤ－ＲＯＭやＣＤ－ＲＯＭあるいはＨＤＤ等の記録媒体５に記録する。そして、この記録媒体５の形で地図データをユーザ側へ提供・配布する。

【００２４】

一方、データ復号化装置２は、外部からのデータを入力するための入力部２１と、その入力部２１を介して入力したデータに対して復号化を施す復号化部２２と、その復号化部２２にて暗号化されたデータを外部へ出力する出力部２３とを備えている。本実施例では、上述の暗号化された地図データを格納した記録媒体５から暗号化された地図データをデータ復号化装置２によって復号化し、その復号化した地図データを例えばカーナビゲーション装置等などのアプリケーション機器７が読み込んで、所定のアプリケーション処理を実行する。例えばカーナビゲーション装置であれば、地図表示や経路探索・表示等の処理である。

【００２５】

上述したデータ暗号化装置１の暗号化部１２及びデータ復号化装置２の復号化部２２は、通常のコンピュータとして構成されており、内部には、周知のＣＰＵ、ＲＯＭ、ＲＡＭ、Ｉ／Ｏおよびこれらの構成を接続するバスラインを備えている。そして、実際の暗号化及び復号化はこれら暗号化部１２及び復号化部２２において実行される。暗号化、復号化には暗号表に当たる「鍵」を使うが、対になる２つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる秘密鍵暗号がある。前者にはＲＳＡ、Ｅｌ Ｇａｍａｌ暗号、楕円曲線暗号などがあり、後者には米国政府標準のＤＥＳ（Data Encryption Standard）や、ＩＤＥＡ、ＦＥＡＬ、ＭＩＳＴＹなどがある。なお、ＤＥＳは、現在では暗号強度が低すぎるため、ＤＥＳの処理を３回繰り返すトリプルＤＥＳといった方式が採用されている。さらに、米国政府の次世代標準暗号化方式であるＡＥＳ（Advanced Encryption Standard）を採用しても良い。

【００２６】

次に、データ暗号化装置１の暗号化部１２において実行される暗号化について説明する。

本実施例における暗号化は、対象となるデータに対し、所定の暗号化単位データ長毎に、その暗号化単位データ長の内で実際に暗号化を施す比率を示す所定の暗号化比率に基づいて、暗号化前後のデータ長が不変の暗号化を施すものである。その具体例を３例示す。

【００２７】

［パターン例１］

図２（ａ）に示す暗号化パターンは、所定の暗号化単位データについて、暗号化部分と非暗号化部分がデータサイズ１：２の比率で形成されるよう、先頭から１／３のみを暗号化する。つまり、先頭から１／３のデータのみが暗号化され、残りの２／３のデータは平文のままである。このような先頭１／３だけの部分的な暗号化が繰り返し実行される。そして、上述のように暗号化前後においてデータ長は不変にされている。

【００２８】

なお、「所定の暗号化単位データ長」があまり長いと、非暗号化部分、すなわち２／３のデータ長分は、暗号化されていない平文のデータが連続してしまうこととなり、不正コピーされた場合に、その連続した平文のデータがそのまま実質的な利用に供される可能性があり、適切な暗号化とは言えなくなる。したがって、不正コピーされた場合において、平文データのみでは実質的に意味をなさない、あるいは利用が非常に制限されてしまうような上限を設定することが好ましい。本実施例では地図データを暗号化対象として考えている。地図データはベクトルデータがメインとなり、また、ある程度広い範囲に対する地図データが平文で存在しなければ、不正コピーしても利用が非常に制限されてしまう。したがって、例えば地図表示をした場合に、実質的に利用できないような表示レベルとなる限度で、暗号化単位データ長の上限を決定すればよい。一方、下限については、不正コピーによる実質的被害の防止のためには暗号化単位データ長は短い方がよいが、短くし過ぎると処理負荷が増大する。そのため、要求される暗号化強度に応じた適切な暗号化単位データ長を採用すればよい。例えば本実施例の地図データの場合であれば、２キロバイト程度を暗号化単位データ長とすることが考えられる。

【００２９】

［パターン例２］

図２（ｂ）に示す暗号化パターンは、複数の暗号化パターンを組み合わせて暗号化していくものである。例えば暗号化単位をデータサイズＳとし、暗号化比率のパターンを３種類（Ｐ１～Ｐ３）準備する。また、１パターンの暗号化をかけるデータサイズをＭ＝ｍ×Ｓとする。

【００３０】

図２（ｂ）に示す具体例は、例えば暗号化単位のデータサイズＳ＝２キロバイト、同じ種類の暗号化パターンを施す繰り返し数ｍ＝２としている。そして、暗号化パターンは以下のようになっている。

Ｐ１：先頭からデータサイズ５０％を暗号化

Ｐ２：先頭からデータサイズ２５％を暗号化

Ｐ３：先頭からデータサイズ７５％を暗号化

したがって、最初及び２番目の暗号化対象のデータＭ１及びＭ２については暗号化パターンＰ１が適用され、３番目及び４番目の暗号化対象のデータＭ３及びＭ４については暗号化パターンＰ２が適用され、５番目及び６番目の暗号化対象のデータＭ５及びＭ６については暗号化パターンＰ３が適用される。そして、７番目及び８番目の暗号化対象のデータＭ７及びＭ８については暗号パターンＰ１が適用され、以下、同様にして暗号化パターンが繰り返し適用されていく。

【００３１】

［パターン例３］

図２（ｂ）に示す暗号化パターンでは、暗号化単位の先頭部分から暗号化を開始しているが、図２（ｃ）に示す暗号化パターンは、暗号化開始位置を変化させている。例えば暗号化単位をデータサイズＳとし、暗号化比率のパターンを３種類（Ｐ11～Ｐ13）準備する。また、１パターンの暗号化をかけるデータサイズをＭ＝ｍ×Ｓとする。そして暗号化パターンＰ11～Ｐ13には、それぞれ暗号化を開始する先頭からの位置も設定する。

【００３２】

図２（ｃ）に示す具体例は、暗号化単位のデータサイズＳ＝２キロバイト、同じ種類の暗号化パターンを施す繰り返し数ｍ＝２としている。そして、暗号化パターンは以下のようになっている。

Ｐ11：先頭２５％位置からデータサイズ５０％を暗号化

Ｐ12：先頭５０％位置からデータサイズ２５％を暗号化

Ｐ13：先頭０％位置からデータサイズ７５％を暗号化

したがって、最初及び２番目の暗号化対象のデータＭ１及びＭ２については暗号化パターンＰ11が適用され、３番目及び４番目の暗号化対象のデータＭ３及びＭ４については暗号化パターンＰ12が適用され、５番目及び６番目の暗号化対象のデータＭ５及びＭ６については暗号化パターンＰ13が適用される。そして、７番目及び８番目の暗号化対象のデータＭ７及びＭ８については暗号パターンＰ11が適用され、以下、同様にして暗号化パターンが繰り返し適用されていく。

【００３３】

このようにデータ暗号化装置１の暗号化部１２において暗号化された地図デー

タは、データ復号化装置２の復号化部２２によって復号化される。復号化部２２は、上述した暗号化時の暗号化ルール及び暗号化に際して用いた暗号鍵を記憶しており、それらに基づいて復号化を実行する。例えば、図２（ａ）に示す暗号化パターンによって暗号化されたデータに対しては、所定の暗号化単位データ長毎に、最初の１／３のデータのみに対して暗号鍵を用いて復号化し、残りの２／３についてはそのまま出力する。

【００３４】

また、図２（ｂ）や図２（ｃ）に示す暗号化パターンによって暗号化する場合であっても同様に、復号化部２２はその暗号化時の暗号化ルール及び暗号化に際して用いた暗号鍵を記憶しており、それらに基づいて復号化を実行する。例えば、図２（ｃ）に示す暗号化パターンによって暗号化されたデータの最初及び２番目の暗号化単位の暗号化対象データＭ１及びＭ２については、次のような処理がなされる。すなわち、最初から２５％のデータサイズ分、つまり０％位置から２５％位置までのデータについては復号化せずにそのままにする。続く５０％のデータサイズ分、つまり２５％位置から７５％位置までのデータについては復号化する。そして、残り２５％のデータサイズ分、つまり７５％位置から１００％位置までのデータについては復号化せずにそのままにする。また、３番目及び４番目の暗号化単位の暗号化対象データＭ３及びＭ４については、最初から５０％のデータサイズ分、つまり０％位置から５０％位置までのデータについては復号化せずにそのままにする。続く２５％のデータサイズ分、つまり５０％位置から７５％位置までのデータについては復号化する。そして、残り２５％のデータサイズ分、つまり７５％位置から１００％位置までのデータについては復号化せずにそのままにする。

【００３５】

以上説明したように、本実施例における暗号化は、対象となるデータを、所定の暗号化単位データ長毎に、所定の暗号化比率に基づいて、暗号化前後のデータ長が不変の暗号化を施す。従来は例えばヘッダ情報のみを暗号化することなどが考えられているが、コンテンツデータについて何ら暗号化されていなければ、そのデータはそのまま利用可能な状態でコピーされてしまう可能性がある。もちろ

ん、ヘッダ情報が暗号化されているため、全く同様に使用することはできなくても、データの内容自体を知ることはできるため、問題がある。それに対して本実施例の場合には、所定の暗号化単位データ中に暗号化されないデータが残存していたとしても、一部は暗号化されているため、所定の暗号化単位データ全体が知られないとデータ内容についての有効利用ができない。また、従来のようにデータ内容に応じて暗号化する場合は、ヘッダ情報がどれかということを解析して判断する必要があるが、本実施例の場合には、暗号化単位データ長と暗号化比率に基づく所定の暗号化ルールに基づいて暗号化するため、データ内容を意識することなく、つまり、どこがヘッダ部分でどこがコンテンツ部分かといった区別をすることなく、所定の暗号化ルールに基づいて機械的に暗号化するだけでよい。そのため、暗号化時における処理負荷の低減が期待できる。

【００３６】

そして、暗号化前後でデータ長が不変であるため、データ復号化装置２においては、復号するために用いる暗号鍵と暗号化のルールを情報として把握していれば、容易に復号化できる。

［その他の実施例など］

（１）上記実施例では暗号化対象のデータをカーナビゲーションシステム等で用いる地図データとして考えたが、地図データに限定はしない。地図データの場合はベクトルデータがメインとなるが、例えば画像データや音声データ、あるいはテキストデータであってもよい。

【００３７】

（２）上記実施例において図２（ｃ）を参照して説明した暗号化パターンは、暗号化比率が２５％、５０％、７５％の３種類、暗号化開始位置が先頭から０％位置、２５％位置、５０％位置の３種類であり、これらを組合せて３種類の暗号化パターンを得た。しかし、これら、３種類の暗号化比率と３種類の暗号化開始位置の組合せによって最大９種類の暗号化パターンを得ることが可能である。例えば暗号化比率が同じ５０％であっても、暗号化開始位置が先頭から０％位置、２５％位置、５０％位置ではそれぞれ暗号化パターンは異なる。そして、このように暗号化パターンが多くなれば、暗号化強度は向上する。

【図面の簡単な説明】

【図１】本発明が適用された実施例のデータ暗号化装置、データ復号化装置の概略構成を表すブロック図である。

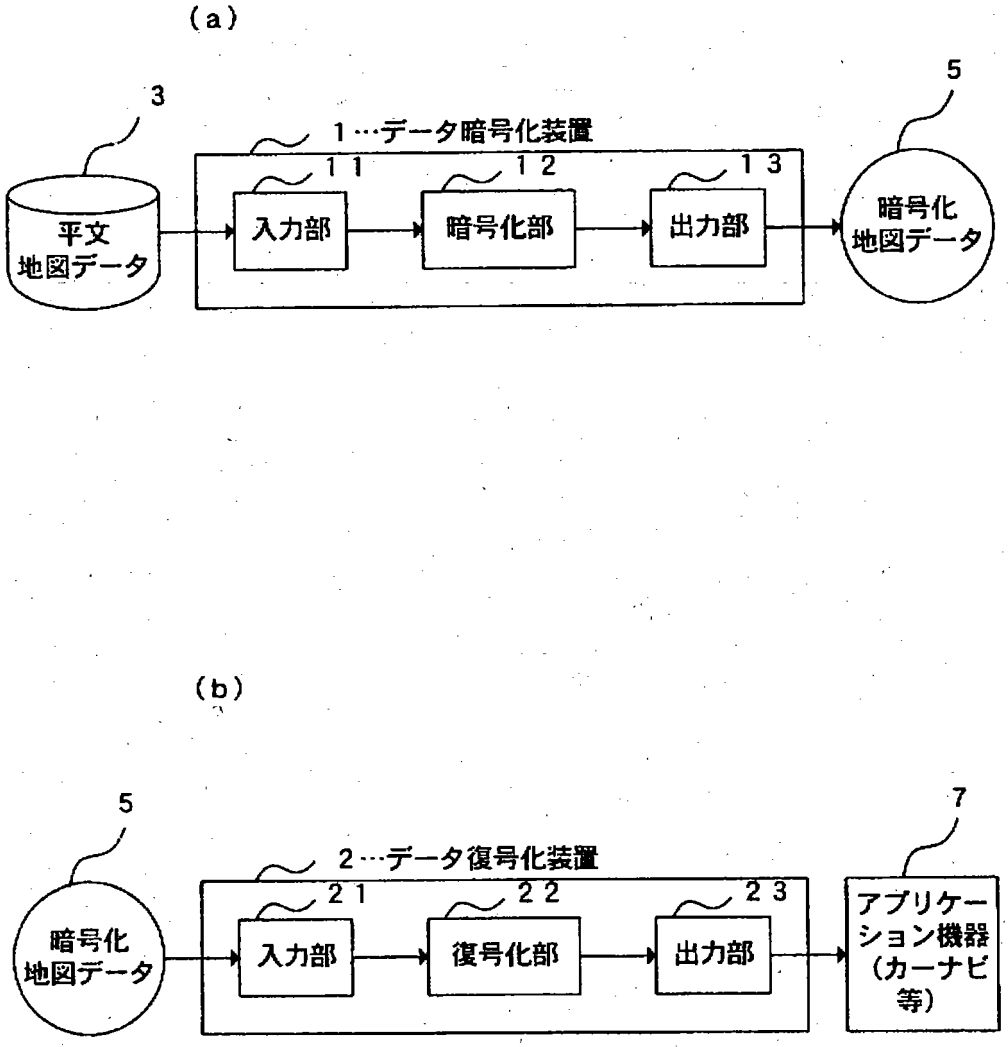
【図２】暗号化のパターン例を示す説明図である。

【符号の説明】

１…データ暗号化装置、２…データ復号化装置、３…データ格納部、５…記録媒体、７…アプリケーション機器、１１…入力部、１２…暗号化部、１３…出力部、２１…入力部、２２…復号化部、２３…出力部。

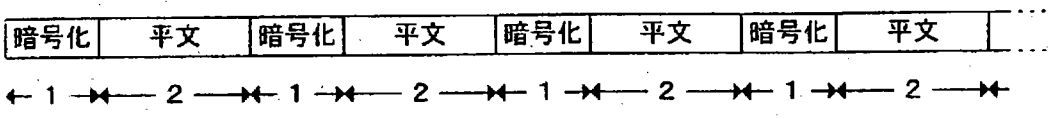
【書類名】　　図面

【図１】


(a)
3
1…データ暗号化装置
11
12
13
5
平文
地図データ
入力部
暗号化部
出力部
暗号化
地図データ
(b)
5
2…データ復号化装置
21
22
23
7
暗号化
地図データ
入力部
復号化部
出力部
アプリケーション機器
(カーナビ等)

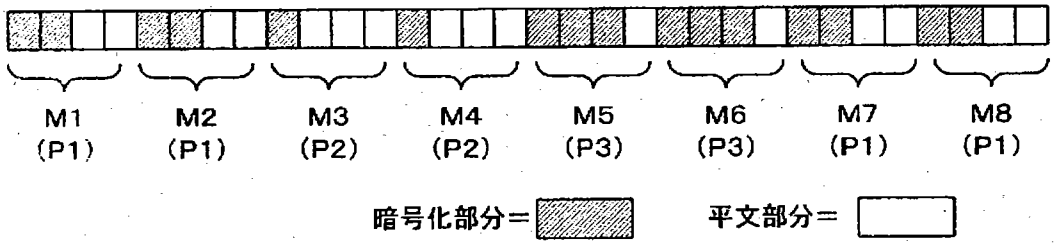
【図２】

(a)



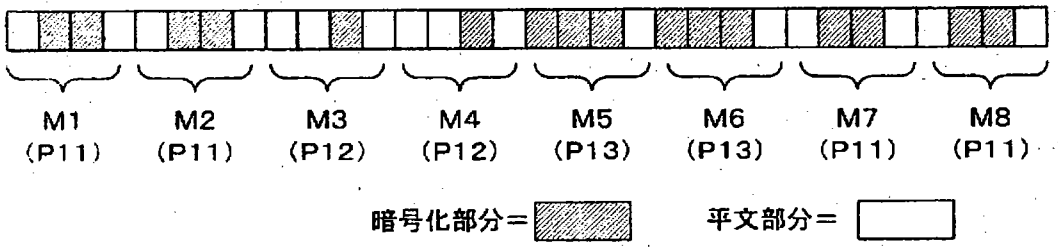
(b)

[暗号化比率パターン]
P1＝50%
P2＝25%
P3＝75%
[繰り返し回数]：2回



(c)

[暗号化比率パターン]
P11＝先頭から25%位置より50%
P12＝先頭から50%位置より25%
P13＝先頭から0%位置より75%
[繰り返し回数]：2回



【書類名】　要約書

【要約】

【課題】不正コピーへの対策を講じながら、復号処理に要する時間を極力低減させる暗号化技術等を提供する。

【解決手段】暗号化単位データ長毎に、暗号化比率に基づいて暗号化前後のデータ長が不変の暗号化を施す。（ａ）の暗号化パターンは、先頭から１／３のみ暗号化し残りの２／３は平文のままとする。（ｂ）の暗号化パターンは、暗号化比率の異なる３種類の暗号化パターンＰ１～Ｐ３を順次適用する。それぞれ先頭からデータサイズ５０％、２５％、７５％を暗号化するパターンである。（ｃ）の暗号化パターンは、さらに暗号化開始位置まで変化させた３種類の暗号化パターンＰ11～Ｐ13を順次適用する。Ｐ11は、先頭２５％位置からデータサイズ５０％を暗号化し、Ｐ12は、先頭５０％位置からデータサイズ２５％を暗号化し、Ｐ13は、先頭０％位置からデータサイズ７５％を暗号化するという内容である。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００４２６０〕

１．変更年月日　　１９９６年１０月　８日
［変更理由］　名称変更
住　所　　愛知県刈谷市昭和町１丁目１番地
氏　名　　株式会社デンソー